The University of Vermont

Responsible Official: Dean of University Libraries and Chief Information Officer

Effective Date: January 11, 2013

University Operating Procedure

Information Security Procedures

Overview

1. **Goal**
   The goal of these Information Security Procedures is to limit information access to authorized users, protect information against unauthorized modification, and ensure that information is accessible when needed, whether that information is stored or transmitted on printed media, on computers, in network services, or on computer storage media.

2. **Application**
   These Procedures apply to all University information maintained in printed form, on computers, through network accounts, via the University e-mail system, or within other information and communication technology services. The Procedures apply whether UVM information resources are accessed remotely or through the use of a University-owned device or UVM network connection.

3. **Guidance vs. Mandates**
   These Procedures contain both rules and guidelines to aid in the interpretation and implementation of the Information Security Policy. In some instances, the Procedures state rules that cannot be implemented immediately but must be implemented over time. Those sections of the Procedures that are presently binding rules employ the conventional language that denotes a mandatory obligation, including words such as "shall," "will" and "must." Those sections that describe recommendations or institutional goals employ language, such as the word "should". With particular reference to detailed technological standards, please contact the Office of the Chief Information Officer, or appropriate officials in Enterprise Technology Services (ETS), for day-to-day guidance about the state of the Procedures' implementation.

4. **Implementation**
   The Procedures are, in essence, a snapshot that reveals both (1) the University's promulgation, implementation, and enforcement of specific standards, and (2) the University's identification of best practices that may not yet be fully implemented. While it remains the University's goal to aggressively pursue the ambitious agenda set forth in these Procedures, full-scale implementation will require a significant transition period. Given the breadth and depth of the territory covered by the Information Security Policy, and the rapidly changing technological and regulatory environment within which we work, a static or wooden presentation of rules is not possible, nor is it fair to expect that all of the principles and goals set forth in these pages could at once be fully operationalized. An example is the laptop encryption standard, section 16.4.2. The University cannot, in one day, encrypt all laptops now in use. However, laptops known to carry Protected University Information must be encrypted immediately, and as University employees or units obtain new laptop computers henceforth, they must all be equipped with encryption software and their users will be bound by the relevant rules. Data Stewards and Technology Managers will define practices appropriate for their domains to implement, over time, these rules and guidelines.

TABLE OF CONTENTS

Summary of Personal Responsibilities and Legal Requirements

In the normal course of business, the University collects, stores, and reports for internal use certain information about individuals that must be kept secure from public disclosure or discussion. That information is stored in a variety of forms – on paper, on desktop and server computer systems, on CDs and tape backup systems – and is transmitted in a variety of ways such as by U.S. mail, intra-campus mail, FAX, e-mail, or web forms. That information has a very real value, and the University has ethical and legal responsibilities, as an institution, for ensuring that policies and procedures are in place to protect those information resources and to secure this information.

The collection, storage, and management of that information is generally the province of the individual administrative or academic offices that use the information. As the steward of the University's enterprise technology resources – central servers and applications systems, networks, telephone systems – Enterprise Technology Services has a key responsibility both to secure the information and systems under its direct control and to establish policies and procedures that guide and support the offices that actually collect and maintain the information. Ultimately, the security of the University's information resources relies upon the actions of individuals who have access to that information. The following section outlines those personal responsibilities.

5. Accountability

All information produced, acquired, or maintained by employees of the University of Vermont in the course of University business is considered University information. Anyone who collects, stores, processes, transfers, administers, or maintains University information is responsible and held accountable for its use.

6. Personal Responsibilities

6.1. Individuals are responsible for their use or misuse of University information.

6.2. Individuals must follow the Privacy Policy and Procedures when Protected Personal Data is accessed. (http://www.uvm.edu/policies/general_html/privacy.pdf)

6.3. No institutional data may be stored unencrypted on non-UVM or personally owned computers, including student employees' computers.

6.4. Bypassing network security provisions that protect UVM's internal network, including establishing wireless systems that access that network, is prohibited.

6.5. Individuals must safeguard all physical keys such as ID cards or electronic tokens, including computer account (NetID) passwords, that provide access to Protected University Information.

6.6. All passwords used for accounts that access enterprise services at the University of Vermont must adhere to UVM password standards for password strength, including password construction and lifetime.

6.7. Individuals must render unusable Protected University Information held on any physical document or computer or computer storage medium that is being discarded.

6.8. Activities that may compromise Protected University Information, or evidence that Protected University Information has been compromised, must be reported promptly in accordance with the Data Breach Notification Policy.

7. Employee Responsibilities

All members of the UVM community are Users of UVM's information resources even if they do not have responsibility for managing information resources. Students, staff, faculty, contractors, consultants, and temporary employees all have access to University information (e.g., file cabinets,

documents, office desks, account passwords) and are responsible for protecting that information wherever it is located. Employees (faculty and staff, student employees, and temporary employees) have special responsibilities because of the access they may have to internal University information resources.

7.1. Individuals are responsible for their use or misuse of Protected University Information. Each individual who has access to information owned by or entrusted to the University is expected to know and understand its security requirements and to take measures to secure the information that are consistent with the requirements defined by its Data Steward, wherever it is located, by locking doors and filing cabinets, protecting account passwords, protecting computer workstations, or encrypting Protected University Information that may be transmitted. Computer workstations must be configured to require username/password on startup. Mobile devices that are used to access any UVM information service other than http://www.uvm.edu must be configured to require a personal identification number (PIN) to unlock and must lock after no more than ten minutes of inactivity.

7.2. Individuals must take appropriate measures to safeguard Protected University Information wherever it is located, such as on physical documents (forms, reports, microfilm/fiche), in filing cabinets, stored on computer media (disks, tapes, CDs/DVDs, USB "thumb" drives), transferred over fax, voice or data networks, exchanged in conversations, etc.

7.3. Individuals must safeguard any physical key, ID card, computer/network account or electronic token that provides access to confidential information. This includes safeguarding computer account (NetID) passwords. Users are personally accountable for all network and systems access under their NetID and must keep their password absolutely secret. Passwords must never be shared with anyone, not even family members, friends, or technology support staff.

7.4. The University provides network file storage for faculty and staff use associated with UVM work, and those systems are backed up automatically. Faculty and staff should use domain-joined file storage for their workstations whenever possible to ensure business continuity in the event of equipment failure, loss, or theft. Employees are responsible for backing up UVM information that has not been stored on automatically-backed-up enterprise network storage.

7.5. Employees must keep work areas clear of confidential materials and configure computer workstations to blank and lockout screens after no more than ten minutes of inactivity, requiring a password to unlock upon return. Employees should consciously activate screensaver/lockout when leaving visual proximity of their workstations.

7.6. To help prevent identity theft, the University requires that its employees take extra precautions when collecting, using, or storing personally identifiable information such as: Social Security Number (SSN), date of birth, place of birth, mother's maiden name, credit card numbers, bank account numbers, or motor vehicle operator's license numbers. These data must be collected or used only for justifiable business needs and only when there is no reasonable alternative. In particular, SSN's should not be used as an internal identifier on forms, reports, screens, etc. Under no circumstances should credit card numbers, SSN, bank account numbers, etc. be exchanged via unencrypted e-mail, since e-mail may be transmitted or stored insecurely. Managers must ensure that their employees understand the need to safeguard this information and that adequate procedures are in place to minimize the risk of disclosure.

7.7. Unencrypted disks, CDs/DVDs, electronic mail (e-mail), electronic chat sessions, instant messages, and unsecured file transfer protocol (FTP) are insecure mechanisms and may not be used to exchange Protected University Information. Any transfer of such information, authorized by its Data Steward, must employ data encryption methods approved by the Information Security Office. Communication involving sensitive, or protected information must use UVM-provided services rather than public systems such as AIM/Yahoo/Google/MS.

7.8. Physical documents, CDs, and DVDs containing Protected University Information secured in locked cabinets or rooms should not be removed from campus. Protected University Information on computer systems or storage devices may be removed from campus only if those devices are encrypted.

7.9. Any University-owned laptop computer used to access UVM non-public data or file services must have its storage system encrypted using a University-approved encryption system, with UVM retaining the encryption key.

7.10. Any personally owned computer system, laptop or desktop, used to access UVM file services or non-public data for anyone other than the individual user must have its storage system encrypted with a system of the owner's choice.

7.11. USB thumb drives, "Secure Disk" or "Compact Flash" drives, CDs/DVDs, PDAs, SmartPhones, etc., that are used to store or transport Protected University Information must be encrypted with University-approved encryption systems.

7.12. Any computer, computer storage system, or removable storage medium that has been used to hold Protected University Information must be physically destroyed or electronically "scrubbed" using software approved by the Information Security Office before being discarded or transferred to any individual or entity not authorized to view the information. The mere deletion of Protected University Information is not sufficient to render it unreadable. Any non-erasable medium (such as CDs or DVDs) that has been used to hold Protected University Information must be physically destroyed before being discarded. The ISO can provide assistance in scrubbing or destroying media.

7.13. Individuals must not in any way divulge, copy, release, sell, loan, review, alter, or destroy any information except as properly authorized within the scope of their professional responsibilities and in accordance with the Records Retention Policy.

7.14. Individuals who are not aware of the security requirements for information to which he or she has access must treat that information as maximally protected until requirements can be ascertained from the appropriate supervisor or Data Steward.

7.15. The sharing of a single network or systems account among a group of individuals is strongly discouraged and should only occur where no reasonable technical alternative is available. Generally, account responsibility should be vested in a single individual.

7.16. Activities that may compromise confidential information must be reported in accordance with the Data Breach Notification Policy.

8. Responsibilities of Deans, Directors, and Department Chairs

Deans, directors, and department chairs are expected to:

8.1. Understand the security-related requirements for information collections used within their respective departments by working with the appropriate Data Stewards and their designees.

8.2. Develop security practices that are consistent with these Information Security Procedures and the Privacy Policy and Procedures that support the University's objectives for confidentiality, integrity, and availability of information as defined by the Data Stewards, and ensure that those procedures are followed.

8.3. Ensure that their staff members have just the minimum access authorizations to information to perform their jobs and ensure that those authorizations are removed (keys returned, security codes changed, computer accounts de-authorized) upon separation from the University or a change in job responsibilities/position. Managers are responsible for administering and retaining written and signed confidentiality agreements for staff from whom those agreements are required by Data Stewards.

8.4. Communicate effectively any restrictions on access or modifications to information to those who use, administer, process, store, or transfer the information in any form.

8.5. Ensure that each staff member understands their information-security-related responsibilities and acknowledges that they intend to comply with those requirements by having staff review the "User responsibilities" in sections 6 and 7.

8.6. Ensure that information and proprietary software are removed from University computers before disposal, whether the equipment is relocated on campus or removed from campus (see section 16.3 of the Operating Procedures below). ETS offers technical advice and tools to assist in removing information (merely deleting is not sufficient!). Physical Plant will pick up computers and ensure environmentally safe disposal.

8.7. Report in accordance with the Data Breach Notification Policy any evidence that information has been compromised or any suspicious activity that could potentially expose, corrupt, or destroy information.

9. Responsibilities of Data Stewards

University-held information must be protected against unauthorized exposure, tampering, loss, and destruction. That information is generally collected, stored, and processed by individual offices that use the paper or computer files in the normal course of business. Each collection is associated with an individual known as a Data Steward who must:

9.1. Define the collection's requirements for security, including confidentiality, integrity, and availability, consistent with these Procedures, the Privacy Policy and Procedures, Records Retention Policy, and other University policies, contractual agreements, laws, and regulations (see section 13, *Asset Classification And Control*);

9.2. Convey the collection's security requirements in writing to the managers of departments that will have access to the collection;

9.3. Work with department heads and chairs to determine the users, groups, roles, or job function that are authorized to access the information in the collection and in what manner (e.g., who can view the information, who can update the information);

9.4. Ensure that contracts with third parties (consultants, service providers) include provisions for maintaining security of information to which they may have access (see model agreements in the Appendices 2, 3 and 4).

Data Stewards may designate one or more individuals to perform the above duties. However, the Steward retains ultimate responsibility for their actions. Section 12.2.3 lists the Data Stewards for major collections of University information.

10. Additional Requirements for Technology Managers

Technology Managers support computing and networking environments where University information is collected, stored, transmitted, or processed. Those environments include:

- Computer servers such as Unix/Linux and Windows servers
- Database environments relying upon database systems such as Oracle, SQL Server, MySQL, Access, Approach, and FileMaker
- Applications environments, both locally and externally hosted, such as PeopleSoft, Banner, Sungard Advance, FAMIS, Kronos, Diebold, Luminis, Digital Measures, PeopleAdmin, Sungard Event Management, and Sungard SmartCall
- Network system components such as routers, switches, and firewalls
- Physical media storage such as tape libraries, file storage systems, and CD/DVD libraries.

Technology managers face more extensive requirements to ensure the security of the technology systems under their management that store and process information, in accord with the Data Steward's definitions, by implementing:

10.1. *Physical security* protection for the equipment for which they are responsible;

10.2. *Computer security* measures for protecting information systems against unauthorized or malicious access or threats posed by computer hackers, including maintaining system security patches and antivirus systems;

10.3. Procedures for administering system and network accounts and access authorizations that satisfy security requirements. For example, for Enterprise information systems, all systems maintenance (device firmware, storage systems, server OS, network devices, network services), and all configuration changes to network topology, firewalls, load balancers, and storage subsystems, shall be approved in advance by the Director of Systems Architecture and Administration or the Director of Telecommunication and Network Services or their designees. Records of the planned changes and the approval of the designated authority shall be maintained for audit purposes; and

10.4. Activity logs for system and network utilization and by monitoring those logs for unusual events that might signal intrusion and access or modification of Protected University Information.

11. Legal Requirements

The University must be mindful of a number of federal and state laws and regulations governing the security of information. The Privacy Policy identifies those laws addressing Protected Personal Data. Those laws as well as additional laws and regulations addressing information security apply across the University and are particularly relevant for certain individual departments and services include the following:

11.1. FERPA (Federal Educational Rights Privacy Act) governs the release of information about students.

11.2. Vermont Act 162 requires that individuals be informed if certain types of personal or financial information are exposed accidentally or through a breach in information security.

11.3. HIPAA (Health Information Portability and Accountability Act) establishes privacy standards for certain health information records. The HITECH (Health Information Technology for Economic and Clinical Health) Act extends the provisions of HIPAA to include new breach notification requirements, establishes requirements for auditing disclosure of information, and increases penalties for violations.

11.4. PCI-DSS (Payment Card Industry – Data Security Standards) is a set of standards required by the payment card industry to help protect credit/debit card information. All "merchants" who process credit cards are required to meet procedural and data security standards.

11.5. GLBA (Gramm-Leach-Bliley Act) requires that all personally identifiable financial information from students, parents, and employees be safeguarded against foreseeable risks of disclosure, intrusion, and systems failure.

11.6. CFAA (Computer Fraud and Abuse Act) makes illegal the use of inter-state or international communications for unauthorized access to "protected computers."

11.7. ECPA (Electronic Communications Privacy Act) prohibits unauthorized access to or disclosure of electronically-stored information, including access by employees to information not within the scope of their duties.

11.8. TEACH (Technology, Education, and Copyright Harmonization) Act allows colleges and universities to use multimedia content for instruction but requires security provisions to ensure that digitally-transmitted content is available only to students who are properly enrolled in the corresponding course.

Operating Procedures: Implementation Details

The following sections provide implementation details associated with the Information Security Policy. The University of Vermont requires all members of the UVM community to manage the information under their control so as to protect that information and ensure its appropriate use, and protecting the information resources of the University. This requirement is embodied in the Information Security Policy, to which these procedures are attached and into which they are incorporated by reference. These procedures may be amended from time to time in response to experience gained or changing circumstances.

12. Organizational Security

All members of the University community share in the responsibility for protecting information resources for which they have access or custodianship. Most of the responsibilities set forth in this section are assigned to four groups of people: Data Stewards, Managers (of Users), Users, and Technology Managers. In general, an individual will have responsibilities in more than one area, for example as both Data Steward and User of information resources and possibly as Manager of a

department. This section also articulates specific responsibilities for the University's Information Security Office, Privacy Office, Audit and Compliance Office, and General Counsel's Office.

12.1. Management Commitment

UVM's Senior Administration commits to securing its information resources by approving this Policy and its Procedures and by charging members of the UVM community to ensure its implementation. It has also instituted senior positions of Privacy Officer, Chief Internal Auditor, and Information Security Officer to verify compliance and update the Policy as legal requirements and best practices evolve.

12.2. Information Security Management

12.2.1. Information Security Program

To promote the security mandate of the University, the University of Vermont:

12.2.1.1. Supports risk management and compliance programs pertaining to information security in compliance with regulations and industry requirements such as FERPA, Vermont Act 162, HIPAA, Gramm-Leach-Bliley, and PCI DSS.

12.2.1.2. Approves and adopts broad information security program principles and seeks to implement best practices in information security.

12.2.1.3. Strives to protect the interests of all stakeholders dependent on information security.

12.2.1.4. Reviews information security policies regarding strategic partners and other third parties.

12.2.1.5. Strives to ensure business continuity.

12.2.1.6. Conducts regular internal and external audits of the information security program.

12.2.1.7. Provides information security metrics to be reported to the Board.

12.2.2. Information security coordination

To promote the security mandate of the University, management shall:

12.2.2.1. Establish information security management policies and controls and monitor compliance.

12.2.2.2. Assign information security roles and responsibilities, set minimum required skills for access, and enforce role-based information access privileges.

12.2.2.3. Assess information risks, establish risk thresholds, and actively manage risk mitigation.

12.2.2.4. Require implementation of information security requirements for strategic partners and other third parties.

12.2.2.5. Identify and classify information assets.

12.2.2.6. Implement and test business continuity and disaster recovery plans.

12.2.2.7. Approve information systems architecture during acquisition, development, operations, and maintenance.

12.2.2.8. Protect the physical safety of information and equipment.

12.2.2.9. Conduct internal and external audits of the information security program with timely follow-up.

12.2.2.10. Collaborate with information security staff to specify the information security metrics to be reported to management.

12.2.3. Allocation of information security roles and responsibilities

To promote the security mandate of the University, the following management roles shall be assigned in writing by the University's President or designee, and appropriate boundaries should be set between these roles; note that some roles could either be combined into one person or be filled by consultants:

Information Security Officer (ISO) has responsibility for the design, implementation, and management of the university's Information Security Program. The ISO promotes a strategic vision for information security, oversees information security policy development and compliance, provides direction on user awareness and education

programming, manages large-scale projects and initiatives as needed, responds to security incidents in coordination with the Chief Privacy Officer, and advises senior management on the risks to University information in the context of regulatory, legal, audit, contractual, and other applicable requirements. The ISO collaborates closely with the Chief Privacy Officer and Chief Information Officer.

Chief Privacy Officer (CPO) Serves as the senior institutional officer for privacy by championing the issue of privacy within the University and promoting the University's commitment to protecting the privacy of personal information. Works proactively with responsible officials to assist in identifying and assessing the effectiveness of University compliance with respect to privacy policies, regulations and laws and promotes strategies to mitigate non-compliance, including assistance with the formulation of standards for the collection, use and sharing of personal information. Acts as a liaison within the institution for privacy issues, including the institutional response to implementing measures responsive to new privacy compliance requirements. This position also serves as the Responsible Official for the Data Breach Notification and Records Retention policies.

Chief Information Officer (CIO) is responsible for maintaining the security of University enterprise information, including the security of enterprise-serving information technology. The CIO also provides leadership for management of information security throughout the decentralized information technology organization.

Chief Internal Auditor is responsible for an independent review and examination of information system records, conducts tests for adequacy of systems controls and compliance with established policy and operational procedures, and recommends indicated changes in controls, policy, and procedures.

Office of the General Counsel is responsible for providing legal advice to the University, reviewing and recommending policy and practice associated with information privacy and security, and assessing the impact of regulations.

Office of Risk Management is responsible for assessing institutional risk associated with contracts, security, and legal issues.

Campus Police are responsible for the public safety and the protection of staff and equipment.

Data Stewards are those persons responsible for ensuring that University Information within their area of assigned responsibility is used with appropriate, controlled levels of access and with assurance of its confidentiality and integrity, in compliance with existing laws, rules, and regulations.

University-held information must be protected against unauthorized exposure, tampering, loss, or destruction. That information is generally collected, stored, and processed by individual offices that use the paper or computer files in the normal course of business. Each collection is associated with a Data Steward who must:

- Define the collection's requirements for security, including confidentiality, integrity, and availability;
- Convey the collection's requirements in writing to the managers of departments that will have access to the collection;
- Work with deans, directors, and department chairs to determine the users, groups, roles, or job functions that are authorized to access the information in the

collection and in what manner (e.g., who can view the information, who can update the information).

- Ensure that contracts with third-party consultants and service providers include terms that provide for the security and confidentiality of the University's information resources.

The term *Data Steward* does not imply ownership in any legal sense, as in holding copyrights or patents. Information stored in libraries, files, and computer systems may be legally owned by others outside the University. In this context, *Steward* simply means the individual with primary responsibility for the security of an information resource acquired or maintained by the University.

Data Stewards may designate one or more individuals on their staff to perform the above duties. However, the Steward retains ultimate responsibility for their actions.

The following table itemizes the categories and data collections and designates the corresponding Data Steward.

Data Steward Designations

Category	Information Pertaining to:	Data Steward
Students	Applicants – undergraduates Applicants – medical students Applicants – non-medical graduate students	Director of Admissions
	Student records – undergraduate Student records – Medicine Student records – Graduate Student records – non-degree courses	Provost, University Registrar, Deans, or Vice President for University Relations and Administration
	Physical health records Mental health records	Director of the Center for Health and Well Being
Instruction	Course materials	Provost, Deans, and Department Heads
Research	Research data and materials	Vice President for Research
Faculty and staff personnel	Applicants Employee data (non-academic information)	Executive Director Human Resource Services and Affirmative Action
	Faculty academic information	Provost
	Dependents and beneficiaries of faculty and staff	Executive Director Benefit and Employee Operations
Alumni and donors	Alumni (personal information) Donors	President and CEO, UVM Foundation
University operations	Academic schools, colleges, and departments and administrative departments	Head of the appropriate unit (dean, director, department head)
	Community affairs	Vice President for University Relations and Administration
	Facilities	Associate Vice President Administrative and Facilities Services
	Financial information, including loans and receivables	Controller, Director of Student Financial Services
	Undergraduate financial aid Medical student financial support Non-medical student graduate student	Director of Student Financial Services

Category	Information Pertaining to:	Data Steward
	financial support	
Public Safety and Law Enforcement	Public safety	Chief of Police Services
Legal Matters	Legal matters	General Counsel
Library Records	Library records	Dean of Libraries

12.2.4. Information Security Advisory Council
An information security advisory council will be appointed by the President or designee to advise the ISO on policy issues and functional security issues and to serve as liaison with the broader University community.

12.2.5. Authorization process for information processing facilities
The establishment of information processing facilities, whether comprised of single or multiple servers or services, must have the express approval of the ISO and be accountable to the ISO.

12.2.6. Externally Hosted Services
Information classified as critical or nonpublic (confidential, departmental, or internal) must not be stored on external services without a contract protecting the University's interests, approved by the ISO.

12.2.7. Specialist information security advice
Contracts or relationships with outside vendors that involve University data or information must be reviewed (or approved) by the ISO.

12.2.8. Co-operation between departments and offices
A comprehensive and effective information security program requires the coordination of all security efforts within the larger institution. All units that provide information technology services must work collaboratively to effect security solutions that are compatible with each other. They must also coordinate their technical and policy decisions with the institutional security program and with the Information Security Officer to ensure that local policies and practices are consistent with the University's Information Security Policy and Procedures.

12.2.9. Independent review of information security
Annual information security audits will be performed by external auditors, either as part of existing financial audits or as established by the ISO. Results of the audit will be presented to the ISO and the Chief Internal Auditor, who will promote corrective action within the organization.

12.2.10. User responsibilities
Users must follow responsibilities outlined in sections 6 and 7 of these Procedures.

12.3. Security of third party access; business agreements
When negotiating contracts with third-party vendors, University officials must consider whether those vendors require access to University files or databases that contain Protected University Information. Agreements with third party vendors or consultants who will have access to such information must specify that the vendor is subject to obligations of confidentiality that will enable the University to continue to comply with its own obligations under applicable laws, and those provisions must survive termination for any reason. In addition, vendors must be contractually obligated to implement data protection and security measures that are commensurate with the University's practices.

Third party access may put information at risk without careful security management. Third parties requesting access to electronic networks, devices, or data must assure compliance with all laws, University policies, and standards including security and privacy, to protect the systems and information.

The ISO examines for risk the proposed access by the third party before approving any access. The granting of access is usually for a limited time and is revocable.

Similarly, University employees must be careful not to disclose confidential information entrusted to their care by an outside party, especially when such information is governed by the terms of a confidentiality agreement or clause ("non-disclosure agreement") with that party.

12.4. Security requirements in outsourcing contracts
Responsibility for overseeing outsourcing contracts resides with senior management including the ISO. The overall vendor program should identify, measure, monitor, and control the risks associated with outsourcing. The contract with third parties must specify the service provider's responsibility for security of the University's resources, protection against unauthorized use, disclosure of any security breaches, compliance with regulatory requirements, and business continuity plans. The contract must include University approval rights for any changes to services, systems, controls, key project personnel or locations of service. The contract must also provide for audits and periodic independent review reports regarding penetration testing, intrusion detection, and firewalls.

12.5. Risk analysis and assessment
An information risk analysis and assessment will be regularly performed in coordination with Internal Audit, Compliance and Privacy Services Office, and the Department of Risk Management and at the direction of the ISO and will become the basis of an Information Security Program or series of Programs.

13. Asset Classification and Control

13.1. Accountability of assets
Data Stewards are responsible for assessing the security requirements for each of their assigned information collections across three areas of concern: confidentiality (in accordance with the Privacy Policy and Procedures), integrity, and availability. To facilitate the assessment process and ensure that these requirements are expressed in a consistent manner across the University, Data Stewards and designates are required to categorize their information collections using the guidelines described in this section.

13.2. Integrity/Availability classifications
Information is assessed as:

13.2.1. *Non-critical* if its unauthorized modification, loss, or destruction would cause little more than temporary inconvenience to the user community or support staff and would incur limited recovery costs. Reasonable measures to protect information considered non-critical would include storing physical information in locked cabinets or office space, using standard access control mechanisms that prevent unauthorized individuals from updating computer information, and making regular backup copies of information files.

13.2.2. *Critical* if its unauthorized modification, loss, or destruction through malicious activity, accident, or irresponsible management could potentially cause the University to:

- Suffer significant financial loss
- Suffer significant damage to its reputation
- Become out of compliance with federal or state legislation
- Adversely impact the University community or its members
- Miss a legally-mandated deadline.

In addition to the protective measures described for non-critical information:

- Samples of critical information must be verified visually or against other sources on a regular basis, and
- A business continuity plan to recover critical information that has been lost or damaged must be developed, documented, deployed, and tested annually.

13.3. Information Classifications

13.3.1. *Protected University Information* (refer to Policy definition) may only be shared on a "need to know" basis with individuals who have been authorized by the appropriate Data Steward, either by their association with specific job functions or by name.

13.3.2. *Departmental* information includes information required for internal operations that may be freely shared with members of the owning department. Sharing such information with individuals outside of the owning department requires authorization by the appropriate Data Steward.

13.3.3. *Internal* or *internal use only* information may be freely shared with members of the University community. Sharing such information with individuals outside of the University community requires authorization by the appropriate Data Steward.

13.3.4. *Public* (refer to Policy definition) information may be shared with individuals on or off campus without further authorization by the Data Steward.

14. Personnel Security

Hiring officials shall determine the extent to which particular positions will require access to nonpublic information and will screen applicants accordingly, as the ability to properly manage and protect information may be an essential function of many University jobs. Hiring officials and supervisors may require the execution of nondisclosure agreements as a condition of employment.

15. Physical and Environmental Security

15.1. Equipment security

Data centers that house enterprise information, personal identity information, or personal health information must be secured with systems that log the identity of individuals entering the facility and maintain video records of activity within the facility. Security protections such as locks, cameras, and alarms must be installed in technology centers and on network distribution closets to discourage and monitor unauthorized access to the physical components in those areas.

Computer systems (servers, desktop and laptop workstations, PDA/SmartPhones), network equipment, network cabling infrastructure, and wireless networking infrastructure must be physically protected commensurate with the level of risk faced by the University should they be compromised. Power, temperature, water, and fire monitoring devices must be deployed as appropriate. Technology Managers are responsible for ensuring that components required to conduct mission-critical business are incorporated into the physical planning for University business continuity.

15.2. General controls

Staff and faculty should file Protected University Information in locked file cabinets when not in active use and should remove such materials from their desks or tables when they leave for meetings or at the end of the day. The security of electronic storage media is discussed in the next section.

16. Security of Employee Computers and Storage Media

16.1. Operational procedures and responsibilities

Individual employees are responsible for implementing the security provisions in this section on the computers and storage media provided to them by the University. Digital storage devices and media that contain Protected University Information must be encrypted, but any written records of encryption passwords must be secured in locked storage. Faculty/staff computer workstations must be configured to blank and lockout screens after no more than ten minutes of inactivity and must require the user's password to re-activate. Those parameters must not be changed by individual users.

16.2. Protection against malicious software

Users may best protect themselves from malicious software by following these directions:

16.2.1. Computer viruses are a major threat to information security. UVM has licensed anti-virus software for University-owned computers where feasible, and anti-virus software

must be installed if available. Download and install virus protection software from the UVM software library at http://www.uvm.edu/software .

16.2.2. Anti-virus software MUST be updated routinely. The easiest way is simply to configure your anti-virus software to update automatically.

16.2.3. Web sites and e-mail attachments are the primary source of computer malware. Avoid web sites that your browser forewarns you might be suspicious. Avoid opening any e-mail attachment unless you were expecting to receive it from that person.

16.2.4. Always virus-scan any files downloaded to your computer from any source (CD/DVD, USB hard disks and memory sticks, network files, e-mail attachments or files from the Internet). Virus scans normally happen automatically, but see the UVM Computing web site, http://www.uvm.edu/it , to learn how to initiate manual scans if you wish to be certain.

16.2.5. Report promptly to the ETS Helpline or through the Data Breach Notification Policy, as applicable, any security incidents in which your computer is known to have been compromised to receive advice on how to minimize the damage.

16.2.6. Respond immediately to any virus warning message on your computer, but do not respond to fake warnings! Warnings that ask you to download software to scan for viruses or pay to have viruses removed are scams and can themselves infect your computer. Only respond to notifications from the virus protection software installed on your computer. If you are in doubt or if you suspect a virus (e.g. by unusual file activity), contact the ETS Helpline. Do not forward any files or upload data onto the network if you suspect your PC might be infected.

16.2.7. Other controls for computers

16.2.7.1. **Prohibited software:** Do not download, install, or use prohibited software programs listed on http://www.uvm.edu/it. Such software could introduce serious security vulnerabilities into UVM's networks or affect the working of your laptop. Software packages that permit the computer to be "remote controlled" (e.g. PCanywhere) and "hacking tools" (e.g. network sniffers and password crackers) are explicitly forbidden on UVM equipment unless they have been explicitly pre-authorized by management for legitimate business purposes.

16.2.7.2. **Backups:** Unless your computer (desktop or laptop) is joined to the CAMPUS domain at UVM, where network-based file services for the *My Documents* folder are backed up automatically by ETS, you must make your own backups of data on your computer – especially important to note for laptops. The simplest way is to logon and upload data from the computer to the network on a regular basis – ideally daily but weekly at least. If you are unable to access the network, it is your responsibility to make regular off-line backups to external hard drives, CD/DVD, USB memory sticks etc. Make sure that off-line backups are encrypted or physically secured. Especially for laptops, remember that if the laptop is stolen, lost or damaged, or simply malfunctions, it may be impossible to retrieve any data from the laptop. Off-line backups will save you a great deal of headache and extra work.

16.3. Disposition of University Computers

Computers that were purchased with University funds or grant funds, donated to the University, or acquired for the University through other means are the property of the University and do not belong to specific individuals. The University must manage surplus computers in an environmentally responsible and fiscally responsible manner that ensures safeguarding of sensitive data and licensed software.

Used computers contain stored data and licensed software that are at risk of unauthorized use. These risks are related to potential violation of software license agreements; unauthorized release of student/patient information; and inadvertent release of NetID and password combinations, financial information, and other personal or sensitive information. All

information must be rendered unreadable and unrecoverable through secure erasure or destruction before any form of disposal, recycling or reuse occurs.

Computers, including monitors, CRTs, CPUs, and related components, contain toxic elements such as lead, cadmium, and other heavy metals that are harmful to the environment when improperly disposed. Computers are prohibited from disposal as solid waste in landfills and as scrap metal in conventional recycling programs.

Owning departments are required to erase data stored on University computers before their relocation, disposal, or transfer to another employee. Enterprise Technology Services (ETS) will offer technical assistance. Physical Plant will pick up computers and ensure environmentally safe disposal.

16.3.1. Information and Software Removal By Departments

Department Chairs, Directors or their designees may declare used computers and related components as "surplus" originating from their department. Before the owning department places a service request to have old computers picked up, it must ensure that all software programs and data files are completely removed.

In this context, "#-Pass Erase" means the number of times a particular program or utility will overwrite random data over a hard drive. The more "passes" run on the hard disk, the more difficult the recovery of documents and files from it. At a minimum, data removal should use a "one-pass zero" method that would be sufficient for most University computers. For greater assurance of erasure, departments may use a software utility that meets or exceed the latest Department of Defense (DoD) standard, which is the currently accepted procedure for data destruction used by the federal government. The original DoD Standard is found at http://www.dtic.mil/whs/directives/corres/pdf/522022p.pdf. The actual method or process for removing institutional data from storage devices is at the discretion of the Data Steward as determined by the nature of the data stored by the User.

For directions on how to properly erase, wipe, or sanitize hard drives and disks, users may visit the Enterprise Technology Services (ETS) Information Security Office website at https://www.uvm.edu/ets/security/erase or contact the ETS Helpline. Instructions are available for both Windows and Macintosh systems. Users need a UVM NetID and password to access this site.

16.3.2. Label Certification for Clean Media

University departments must certify that all data and software have been removed from computers before turning them over to the Physical Plant Department. Each machine must display a *Certified Clean Media to be Recycled* label that provides information about who cleaned the machine, the department, on what date, and the method or program used. A template for labels is available on the Enterprise Technology Services (ETS) Information Security Office website at: https://www.uvm.edu/ets/security/erase. Labels may also be requested from UVM Physical Plant Recycling Office.

16.3.3. Redeployment of Surplus Computers

Department chairs, directors, or their designees may allow redeployment of surplus computers in the following instances.

16.3.3.1. Transfer internally to another University department or user. The original owning department must ensure that the disk is erased and the operating system (or current version of the original operating system, if appropriately licensed) is reinstalled before transfer.

16.3.3.2. Allow an individual employee to take their old University computer for personal use if the computer cannot be redeployed within the department,

subject to the Moveable Equipment policy which applies to equipment over $5,000, and, for equipment under that threshold that is purchased on a grant, subject to the terms and conditions of the grant. The owning department must ensure that the disk has been erased and that the operating system and bundled software has been reinstalled before transfer. After the hard drive has been erased, when transferring for personal use, the owning department may only reinstall the original operating system software that was licensed with the original computer. See the UVM Computing web site, http://www.uvm.edu/it , for information.

16.3.3.3. Donate a computer to a recognized 501(c)(3) charitable organization such as a school, religious institution, or similar non-profit. The owning department must coordinate the details of the exchange and receive proof of 501(c)(3) status of recipient. The owning department must ensure that the disk has been erased and that the original licensed operating system and bundled software has been reinstalled before transfer. After the hard drive has been erased, the owning department may only reinstall the original operating system software that was licensed with the original computer. See the UVM Computing web site, http://www.uvm.edu/it , for information.

16.3.4. Disposition of Computers By Physical Plant

All surplus computers that have not been redeployed through one of the above instances must be delivered to the Physical Plant Department for proper recycling and disposal. Owning departments must submit a Service Request using the FAMIS Self-Serve system to request a pickup of surplus computers and components. All equipment must be unplugged and disconnected before pick-up. All equipment must display a completed *Certified Clean Media to be Recycled* label. Physical Plant will ensure environmentally safe disposal through a certified electronics recycling and disassembly facility.

16.3.5. Anti-Scavenging

Unauthorized removal, transfer, or disposal of University owned property, regardless of value, is considered theft and constitutes a serious breach of these Procedures.

To submit a Service Request to Physical Plant department to request pickup of surplus computers, go to the FAMIS Self Service site at http://www.uvm.edu/fss or contact Physical Plant Service Operations Support at (802) 656-2560. Users may also contact the Physical Plant Department's Recycling & Solid Waste Supervisor, 284 East Avenue, (802) 656-4191.

16.4. Laptop Security

Portable computers are especially vulnerable to physical damage or loss, and to theft, either for resale or for the information they contain. The impact of such losses includes not just the replacement value of the hardware but also the value of any UVM or personal data on or accessible through them. Information is a vital UVM asset. The impacts of unauthorized access to, or modification of, important or sensitive UVM data can far outweigh the cost of the equipment itself.

16.4.1. Physical security controls for laptops

Users may best protect their laptops by following these directions:

16.4.1.1. The physical security of "your" laptop is your personal responsibility so please take all reasonable precautions. Stay alert to the risks.

16.4.1.2. Keep your laptop in your possession and within sight whenever possible, just as if it were your wallet, handbag or mobile phone. Be extra careful in public places such as airports, railway stations or restaurants. It takes thieves just a fraction of a second to steal an unattended laptop.

16.4.1.3. If you have to leave the laptop temporarily unattended in an office, meeting room, or hotel room, even for a short while, shut the system down and use a

laptop security cable or similar device to attach it firmly to a desk or similar heavy furniture. These locks are not very secure but deter casual thieves.

16.4.1.4. Never leave a laptop visibly unattended in a vehicle. If absolutely necessary, lock it out of sight in the trunk or glove box, but it is generally much safer to take it with you. Lock the laptop away out of sight when you are in an unfamiliar location (e.g., hotel), preferably in a strong cupboard, filing cabinet or safe.

16.4.1.5. Carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage. An ordinary-looking briefcase is also less likely to attract thieves than an obvious laptop bag.

16.4.1.6. Keep a note of the make, model, serial number, Ethernet MAC address, and wireless MAC address of your laptop, but do not keep this information with the laptop. If the laptop is lost or stolen, notify UVM Police immediately and contact the UVM Information Security Office (ISO@uvm.edu) as soon as possible (within hours if not minutes).

16.4.1.7. If you are traveling abroad with a laptop or mobile storage device, investigate whether local laws might put information you're carrying at risk.

16.4.2. Controls against unauthorized access to laptop data

16.4.2.1. You must use approved encryption software on all UVM laptops, choose a long, strong encryption password/phrase, and keep the password secure. See the UVM Computing web site, http://www.uvm.edu/it , for further information on laptop encryption. If your laptop is lost or stolen, encryption provides very strong protection against unauthorized access to the data.

16.4.2.2. UVM laptops are provided for official use by authorized faculty and staff. Do not loan your laptop or allow it to be used by others such as family or friends.

16.4.2.3. Do not leave your laptop unattended and logged on. Always shut down, log off, or activate a password-protected screensaver before walking away from the machine.

16.5. Campus network management

16.5.1. Network controls (RESERVED)

16.6. Exchange of information and software

To reinforce workstation security best practices, members of the UVM community should not generate mass e-mails that include attachments. Rather, materials should be included as text in the message (for short messages) or linked *as text, not hyperlink*, to a web site that provides the document for download (longer messages) so that members of the UVM community do not become accustomed to simply clicking on attachments or links. Computer workstation internal firewalls must be configured to reject all incoming connection attempts except those for which the user has installed applications that require specific ports to be available.

16.7. Responding to security incidents and malfunctions

In the event of a security incident or perceived system malfunction related to security management, refer to http://www.uvm.edu/it/security for guidance on reporting security incidents. Potential breaches of sensitive data should be reported in accordance with the Data Breach Notification policy. Prompt action may be critical. Disconnect the computer from the network but leave the system powered on and running. Information from the running system may be needed to manage the incident or to comply with legal requirements. After reporting, do not take any further action.

17. Access Control

Technology Managers must take steps to protect their servers and mainframes from compromise by either external agents or members of the UVM community. They must select operating systems and other software that is inherently securable, modify default passwords immediately upon installation, and establish firewall and other system configuration parameters to minimize vulnerabilities. They must install operating system and application security patches promptly. They must monitor and verify system access logs routinely and monitor performance data for signs of unauthorized access

and systems compromises. They must cooperate with and assist Enterprise Technology Services in performing independent evaluations of system security for both internal and external audits.

These responsibilities also apply to individuals who install software, scripts, or other applications that are accessible from internal or external networks, whether the applications are running on University servers (such as in a "shell" account or web site) or on desktop or laptop workstations.

17.1. Access control policy
Remote access to a particular computer or device on the University internal network can compromise access to other computers, storage systems, and applications on the network and must be approved by the ISO Team. Dial-in modems and wireless systems expose the University's internal information systems to security compromises, and their use on UVM's internal network (outside Residence Life) is prohibited without explicit authorization by Telecommunications and Network Services.

17.2. Identity management
17.2.1. Departments should use central authentication services (NetID) to control access to their applications whenever possible.
17.2.2. Departments that operate authentication services must meet ETS strength requirements at a minimum.
17.2.3. Departments that employ external services for applications support should include the availability of Federated ID as an RFP requirement for vendors. If such services are not available, vendors will be required to use UVM's LDAP authentication system. In no case should UVM offices contract for external applications services that maintain individual, independent account names and passwords without authorization from the ISO.

17.3. User responsibilities
Many personal computer operating systems can be configured to allow access across the Internet. Server "shell" accounts may allow user installation of software that can be used by people other than the account holder. Web sites may run scripts and other software not provided or tested by University technology managers. Individuals must take care to ensure that their computer systems and installed software are configured to prevent unauthorized access. When remote access is allowed, special care must be taken to select safe implementation options and ensure that passwords and other access controls are secure. Individuals must stay informed about vulnerabilities in applications, scripts, operating systems and other software they are using or making available, keeping them updated with security fixes or disabling their use if fixes are not available or not applied.

17.4. Network access control
Service Providers who support authorized access to University information must implement designs, policies, and procedures that protect the integrity of the University's network and service architecture. Network security is maintained through a combination of technologies, including switched networks, strong authentication, encryption, firewalls, and access controls. All Service Providers must respect the University physical network strategy and deploy UVM-standard equipment. Network access, including modem, remote desktop access, and wireless access, must be implemented using UVM standards and with explicit written authorization by Telecommunications and Network Services.
17.4.1. Policy on use of network services (RESERVED)
17.4.2. Enforced path (RESERVED)
17.4.3. User authentication for external connections
Access to files on UVM's internal network containing nonpublic information will be permitted only via VPN or securely authenticated and encrypted file services.
17.4.4. Node authentication (RESERVED)
17.4.5. Protection from malicious network access
Because the loss of integrity on any device or server on UVM's internal network provides a platform for launching attacks on the integrity of the entire network, ETS will periodically scan and probe the network, network servers, individual computers,

and other devices for vulnerabilities using software tools designed for that purpose. Service Providers and others responsible for network-attached systems are required to participate in and support the security diagnostic processes, review resulting vulnerability reports, and act on them to eliminate security vulnerabilities.

17.4.6. Separation of duties and least privilege
In assigning access privileges to information sources, UVM will adhere to the model of least privilege. Separation of duties will be employed whenever feasible to limit the chance of unauthorized data modification or other fraudulent activities.

17.4.7. Network connection protocols (RESERVED)

17.4.8. Network routing control (RESERVED)

17.4.9. Security of network services – authority for devices
Telecommunications and Network Services will disconnect from the network any servers or workstations with Protected University Information that fail to pass security scans and other devices that might allow UVM's internal network to be compromised. If necessary, the connecting network segment may be isolated from the campus network until the failing device can be identified and isolated.

17.4.10. Firewall Waivers (RESERVED)

17.5. Net IDs and Passwords
Net ID-password identity pairs maintained by UVM's Enterprise Technology Services represent the electronic identities of individuals and are used to access a variety of centrally managed information resources at UVM, ranging from personal payroll or student records information, through class or benefits enrollment, to access to software licensed for campus use. The NetID-password identity pairs may also be used by departmental services or external services that are able to use the enterprise authentication system.

All passwords used for accounts that access enterprise services at the University of Vermont must adhere to UVM password standards for password strength, including password construction and lifetime. These standards are set forth in the following section.

17.6. Password Standards
Passwords for newly activated accounts must be set at first use to ensure that only the person to whom the account has been issued knows the password and has access to the account. NetID owners must agree to comply with UVM's Acceptable Use Policy before activating their accounts.

UVM uses a self-selection system through which clients select their own passwords, and accordingly, clients have responsibilities associated with those passwords:

17.6.1. Password Construction

17.6.1.1. Passwords must be at least eight characters in length.

17.6.1.2. Passwords must contain at least two of the four types of character groups (UPPER CASE, lower case, digits 0-9, and special [$#-_!]).

17.6.1.3. Passwords cannot be based upon words that can be found in a dictionary.

17.6.2. Password Aging and Changing
Passwords must be changed every twelve months; changes every 60 days are recommended. Passwords may be changed by visiting the web site https://www.uvm.edu/account

17.6.2.1. UVM will enforce annual password changes by suspending, with forewarning, accounts for which passwords have not changed in twelve months or more. UVM will also suspend accounts that appear to be targets of break-in attempts (repeated failed login attempts) or are used for activities that violate this or other University policies.

17.6.2.2. Clients should change their passwords immediately if it appears that account security might have been compromised, as, for example, if the NetID/password combination had been used on a workstation that was subsequently discovered to have a keylogger virus, or if the password had

been entered on a computer, PDA, phone, or similar mobile device that was subsequently lost or stolen.

17.6.3. Individual Responsibility

17.6.3.1. Only the individual may activate the NetID they have been assigned or change its password.

17.6.3.2. Passwords provide access to personal information and may provide access to personal information of other UVM constituents. Individuals are responsible for actions performed in their names within their accounts and thus are responsible for securing access keys. Do not share passwords or the information you use to construct it with anyone, including UVM officials or technical support staff. Report requests for your password to UVM ETS Account Services.

17.6.3.3. Passwords should not be written and left as Post-Its on displays, under keyboards, or in or on desks. Protect them as you would a bank PIN.

17.6.3.4. Store passwords in a computer file only if the file is encrypted.

17.6.3.5. Do not allow web browsers or e-mail programs to "remember" passwords on workstations other than your own encrypted system.

17.6.3.6. Use non-UVM password storage systems only if the system encrypts its data in such a manner that only you can retrieve them.

17.6.3.7. Do not enter UVM NetID/password into non-UVM systems to access UVM services (e.g., groovyuv.com for UVM webmail).

17.6.3.8. Do not use UVM NetID and password when creating accounts on non-UVM systems, since the managers of those systems might attempt to use that information to access your UVM account or might not store passwords securely.

17.6.4. System Requirements

17.6.4.1. Automatic Lockout

One way to secure account access from automated password cracking systems is to automatically lock out accounts after a limited number of unsuccessful login attempts. Automatic lockout is a requirement in information security standards. Because of the distributed nature of UVM's systems and client systems' inability to relay failed-login messages from authentication systems, UVM cannot immediately implement universal automatic lockout on all enterprise systems. However, as opportunities arise in applications that do support automatic lockout, UVM will implement that capability.

17.6.4.2. Transmission of NetID and Passwords

UVM's enterprise systems will not transmit NetID/password pairs as clear text.

17.6.4.3. System-Based Password Files

UVM's enterprise systems do not use system-based password files, and central authentication NetID/passwords are not distributed to non-ETS systems. Password processing for authentication should always use ETS-managed central authentication based on Kerberos, LDAP, Shibboleth Federated ID, or Windows Active Directory.

17.6.4.4. Auditing and Testing

The Internal Auditor or designee may periodically request reports to document that passwords are being changed routinely, as required, and that dormant accounts have been suspended and then terminated. The code that supports password changing may be audited periodically to ensure that it is enforcing the policy documented here.

17.6.5. Access Limitations

17.6.5.1. Access to enterprise accounts will normally be terminated when individuals no longer meet the criteria for which they were granted access initially

(https://www.uvm.edu/ets/security/?Page=when-employee-leaves.html). Termination of employment, for example, normally results in termination of enterprise accounts. Exceptions are generally granted, as account suspensions, when the individual's association with the University is cyclic (e.g., part-time faculty who teach occasionally). ETS Account Services may terminate enterprise accounts by locking them against further access.

17.6.5.2. ETS Account Services, Systems Architecture and Administration, or automated lockout systems may also disable enterprise accounts by locking the account in order to resolve possible account abuses or security breaches.

17.6.5.3. *Affiliated organization* employees are research associates or contracted consultants working with or for UVM faculty or staff. In some instances they may be granted enterprise accounts to gain access to UVM resources needed to conduct their work. Their accounts are normally terminated when ETS's Account Services learns that their association with UVM has ended. Their accounts will be reviewed semi-annually through this password management process in any case.

17.6.5.4. Non-enterprise systems that do not use enterprise NetID/password for authentication/authorization and that do not manage access control as documented above should be reviewed for inclusion in the enterprise authentication system.

17.6.6. Third Party Access

17.6.6.1. Use of the UVM electronic identity system by third-party and off-campus organization is encouraged and supported in order to improve service and security for services provided to members of the UVM community. UVM will seek opportunities to use Federated Identity systems to secure access to third-party services on behalf of UVM clients.

17.6.6.2. Other third-party and off-campus use of NetID/password for authentication of UVM identities is explicitly prohibited without prior agreement of the Director of Systems Architecture and Administration.

17.7. Operating system access control

17.7.1. Password management system

The University has implemented mechanisms to ensure strong password security, including password strength assurances and periodically-required routine password changes approaching NIST Level of Assurance 2 for password security. Whenever possible, Technology Managers should employ that system, available via LDAP or Shibboleth Federated ID, for password management. In cases in which that is not possible because of local applications software, Managers should implement equivalent password security measures on local systems.

System administrators must have access to reset passwords of clients but should never have access to view them.

17.7.2. Use of system utilities (RESERVED)

17.7.3. Session time-out

Session time-outs may be as long as eight hours for open applications sessions that might corrupt database applications if closed, provided that client workstations have screen-blanking timeouts enabled for ten minutes of inactivity as required by Section 16.1.

17.7.4. Limitation of connection time (RESERVED)

17.8. Application access control (RESERVED)

17.9. Monitoring system access and use (RESERVED)

17.10. Telecommuting and use of personal equipment

17.10.1. Only the employee may have administrative rights on personal equipment used to manage enterprise information resources.

17.10.2. Virus protection must be used at least for Windows systems and at the employee's expense if on personal equipment.
17.10.3. Operating system automatic updates must be enabled.
17.10.4. No software may be installed on personal equipment that is not allowed on UVM-owned computers (as determined by the ISO).
17.10.5. Operating system firewall must be enabled.
17.10.6. Home network hardware (NAT) firewall is encouraged.
17.10.7. Protected University Information, and information that is protected by law, professional ethics standards, or University policy, may not be stored unencrypted, including unencrypted email.
17.10.8. UVM credentials must not be transmitted unencrypted.

18. System Development and Maintenance

18.1. Security requirements of systems (RESERVED)
18.2. Security in application systems
Technology Managers who develop, maintain, or modify key applications relating to student records, human resource information, or financial records must deploy adequate procedures for managing change control, separation of test and production environments, and separation of responsibilities and authorizations for staff involved in those functions. These procedures will assist Internal Audit, Compliance and Privacy Services, and the Information Security Office in ensuring that policies are respected and adequate procedures are in place.
18.3. Cryptographic controls (RESERVED)
18.4. Security of system files (RESERVED)
18.5. Security in development and support process
Real data used in pre-production development and testing systems must be secured to the same extent that production systems are secured.

19. Business Continuity Management (Disaster Recovery) (RESERVED)

Definitions

Protected University Information includes both Protected Personal Data and Sensitive University Information as defined below:

- ***Protected Personal Data (PPD)*** includes, without limitation, personally identifiable information, protected health information, and protected student information as described below. Protected University Data includes data maintained in any electronic or hard copy medium. *Note*: Potential breaches of Protected Personal Data (PPD) must be reported in accordance with the Data Breach Notification Protocol (http://www.uvm.edu/policies/general_html/databreach.pdf).
    - *Personally Identifiable Information (PII)*– under 9 V.S.A. §2430(5) is defined as an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized person:
        - Social Security number;
        - Motor vehicle operator's license number or non-driver identification card number;
        - Financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords;
        - Account passwords or personal identification numbers or other access codes for a financial account.

- *Protected Health Information (PHI)* includes identifiable health information as defined at 45 CFR §160.103 that is transmitted or maintained by the University's covered HIPAA components; PHI also includes identifiable health information that is obtained by a University member pursuant to an agreement with another organization or governmental entity and which is protected under the HIPAA/HITECH Act.
- *Protected Student Information* – Student education records maintained by the University, whether by academic or administrative units, and protected under the Family Educational Rights and Privacy Act (FERPA) and as described more fully in the UVM FERPA Rights Disclosure policy (http://www.uvm.edu/policies/student/ferpa.pdf).

- ***Sensitive University Information*** about the University, or University property or information regarding individuals not identified as PPD, that includes, without limitation, information involving certain legal matters, or business and financial transactions, grant applications, pending patent applications, institutional electronic security architecture, and information about security breaches or other events.

Authorized Users: Individuals – faculty, students, staff, or affiliates – who have been issued a UVM NetID and are authorized to access specific information resources in order to perform business functions for the University or in order to conduct business with the University.

Data Destruction: Any physical, chemical, or electronic process that alters magnetic, electronic, paper, CD, DVD, or other forms of data storage in a manner that renders the data permanently and irretrievably unreadable.

Data Stewards: Members of the University community who have the operational responsibility for particular collections of information such as student, employee, or alumni records (collection(s)).

NetID or Network Account: The electronic identity managed by Enterprise Technology Services that is provided for each member of the University community to access University Information Systems, including internal electronic information services.

Password: A carefully constructed confidential character string used to validate individuals for access to University Information Systems, specifically, network accounts.

Public information: Information that may be disclosed to any person inside or outside the University. Although such information may be made public, precautions may still be required to protect against unauthorized or malicious modification or destruction.

Technology Managers: Individuals who develop, implement, or maintain information systems or who have privileged access to information technology systems such as servers, networking equipment, and personal workstations in order to manage or support development on those systems, whether those systems are housed in UVM facilities or hosted externally.

University Employees: Student employees, staff, faculty, contractors, consultants, temporary employees and affiliates of the University of Vermont.

University Information: Information in any form and recorded on any media that the University or its agents use or create in the course of conducting University business, including research and teaching activities, except those materials specifically excluded from University ownership as set forth in the University's Intellectual Property Policy.

University Information Systems: Electronic or physical University or externally-hosted systems that are used to collect, store or transmit information, including, without limitation, email, University-owned

computers, communications equipment and software, University network accounts, file cabinets, storage cupboards, and internal mail or delivery systems.

Users: Individuals who use University Information or University Information Systems, even if they do not have responsibility for managing institutional resources.

Contacts/Responsible Official

Questions related to the daily operational interpretation of this policy should be directed to the individuals listed below.

For questions related to Information Security:

Chief Information Officer
234 Waterman Building
85 S. Prospect Street
University of Vermont
Burlington, Vermont 05405
(802) 656-4900
cio@uvm.edu

The Dean of University Libraries and Chief Information Officer is the official responsible for interpretation and administration of this procedure.

Related Documents/Policies

Code of Conduct and Ethical Standards
http://www.uvm.edu/~uvmppg/ppg/general_html/businessconduct.pdf
Computer, Communication, and Network Technology Acceptable Use
http://www.uvm.edu/policies/cit/compuse.pdf
Data Breach Notification Policy
http://www.uvm.edu/policies/general_html/databreach.pdf
Disposal of Surplus Property and Movable Equipment
http://www.uvm.edu/policies/facil/surplusdisposal.pdf
FERPA Rights Disclosure Policy
http://www.uvm.edu/~uvmppg/ppg/student/ferpa.pdf
Information Security Policy
http://www.uvm.edu/policies/cit/infosecurity.pdf
Intellectual Property Policy
http://www.uvm.edu/~uvmppg/ppg/general_html/intellectualproperty.pdf
Privacy
http://www.uvm.edu/policies/general_html/privacy.pdf
Records and Documents Requests Policy
http://www.uvm.edu/~uvmppg/ppg/general_html/record_request.pdf
Records Retention Policy
http://www.uvm.edu/~uvmppg/ppg/general_html/recordretention.pdf
Subpoenas, Complaints, Warrants and other Legal Documents
http://www.uvm.edu/policies/general_html/subpoenas.pdf
University Sponsored Social Media
http://www.uvm.edu/policies/cit/socialmedia.pdf

Effective Date

Approved by the Responsible Official January 11, 2013.

Appendix 1: Securing Protected University Information – Summary of Responsibilities

The University of Vermont possesses information that is sensitive and valuable, e.g., personally identifiable information, financial data, building plans, research, and other information considered sensitive. Some information is protected by federal and state laws or contractual obligations that prohibit its unauthorized use or disclosure. The exposure of sensitive information to unauthorized individuals could cause irreparable harm to the University or members of the University community, and could also subject the University to fines or other government sanctions. Additionally, if University information were tampered with or made unavailable, it could impair the University's ability to do business. The University therefore requires all employees to diligently protect information as appropriate for its sensitivity level.

Failure to comply with this policy may subject you to disciplinary measures. For University employees, failure to comply may result in termination.

1. Responsibilities of All Employees and Contractors

1.1. You may only access information needed to perform your legitimate duties as a University employee and only when authorized by the appropriate Data Steward or designee.

1.2. You are expected to ascertain and understand the sensitivity level of information to which you have access through training, other resources, or by consultation with your manager or the Data Steward.

1.3. You may not in any way divulge, copy, release, sell, loan, alter or destroy any information except as authorized by the Data Steward within the scope of your professional activities.

1.4. You must understand and comply with the University's requirements related to Protected University Information.

1.5. You must adhere to University's requirements for protecting any computer used to conduct University business regardless of the sensitivity level of the information held on that system.

1.6. You must protect the confidentiality, integrity and availability of the University's information as appropriate for the information's sensitivity level, wherever the information is located, e.g., held on physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation, etc.

1.7. Information deemed Protected University Information under this policy must be handled in accordance with the University's requirements for protecting confidential and highly confidential information.

1.8. You must safeguard any physical key, ID card or computer/network account that allows you to access University information. This includes creating difficult-to-guess computer passwords.

1.9. You must destroy or render unusable any Protected University Information contained in any physical document (e.g., memos, reports, microfilm, microfiche) or any electronic, magnetic or optical storage medium (e.g., USB key, CD, hard disk, magnetic tape, diskette) before it is discarded.

1.10. You must report any activities that you suspect may compromise sensitive information to your supervisor and to the University Information Security Office.

1.11. Your obligation to protect sensitive information continues after you leave the University.

1.12. While many federal and state laws create exceptions allowing for the disclosure of confidential information in order to comply with investigative subpoenas, court orders and other compulsory requests from law enforcement agencies, anyone who receives such compulsory requests must contact the Office of the General Counsel before taking any action.

1.13. If you are performing work in an office that handles information subject to specific security regulations, you will be required to acknowledge that you have read, understand and agree to comply with the terms of this policy annually.

2. Responsibilities of Managers and Supervisors

In addition to complying with the requirements listed above for all employees and contractors, managers and supervisors must:

2.1. Ensure that departmental procedures support the objectives of confidentiality, integrity and availability defined by the Data Stewards and designees, and that those procedures are followed.

2.2. Ensure that restrictions are effectively communicated to those who use, administer, capture, store, process or transfer the information in any form, physical or electronic.

2.3. Ensure that each staff member understands his or her information security-related responsibilities.

3. Responsibilities of Technology Managers

In addition to complying with the policy requirements defined for all employees and contractors, and managers and supervisors, those who manage computing and network environments that capture, store, process and/or transmit University information, are responsible for ensuring that the requirements for confidentiality, integrity and availability as defined by the appropriate Data Steward are being satisfied within their environments. This includes:

3.1. Understanding the sensitivity level of the information that will be captured by, stored within, processed by, and/or transmitted through their technologies.

3.2. Developing, implementing, operating and maintaining a secure technology environment that includes:

a. Implementing a cohesive systems architecture,
b. Adhering to product implementation and configuration standards,
c. Follow procedures and guidelines for administering network and system accounts and access privileges in a manner that satisfies the security requirements defined by the Data Stewards, and
d. Implementing an effective strategy for protecting information against generic threats posed by computer hackers that adheres to industry-accepted "best practices" for the technology.

3.3. Ensuring that staff members understand the sensitivity levels of the data being handled and the measures used to secure it.

4. Responsibilities of Data Stewards

In addition to complying with the requirements listed above, Data Stewards are responsible for:

4.1. Working with the University Information Security Office and the Office of the General Counsel to understand the restrictions on the access and use of information as defined by federal and state laws and contractual obligations.

4.2. Segregating the information for which they are responsible into logical groupings, called information collections.

4.3. Defining the confidentiality, integrity, availability, longevity and destruction requirements (sensitivity level) for each of their information collections.

4.4. Conveying in writing the sensitivity level of each information collection for which they are responsible to the managers of departments that will have access to the collection,

4.5. Working with department managers to determine what users, groups, roles or job functions will be authorized to access the information collection and in what manner (e.g., who can view the information, who can update the information).

4.6. Ensuring that contracts with third-party contractors include provisions for maintaining the security and confidentiality of the University’s information resources and for properly destroying or returning records at the end of the contract.

Appendix 2: Protected University Information Agreement for Vendor Remote or On-Site Support

The form on the following page (or a comparable form approved by the Office of General Counsel) must be signed by an appropriate representative of any external organization before any member of that organization can gain access to University computer systems that contain Protected University Information.

Protected University Information Agreement – Vendor Remote or On-Site Support

This agreement is hereby entered into, by and between _____ _____(hereinafter "Service Organization") and the University of Vermont (hereinafter "UVM") on __(date).

UVM and Service Organization mutually agree to the terms of this Agreement to govern the handling of UVM data and information by any employee, subcontractor, agent or other individual affiliated with Service Organization (hereinafter "Service Provider") to which he or she may have access during the course of any work done relating to the maintenance, support or testing of computer software and/or hardware used by UVM.

If any conflict exists between the terms of this agreement and any prior agreement, the terms of this agreement shall govern.

1. Definitions:

   The term *Service Provider* will refer to any employee, subcontractor, agent or other individual affiliated with Service Organization who has access to UVM data and information.

   The term *Covered Data and Information* will refer to any piece of UVM data and information to which any Service Provider may have access during the course of his or her performing work relating to the maintenance, support or testing of computer software and/or hardware used by UVM.

2. Acknowledgment of Access to Covered Data and Information: Service Organization acknowledges that the Agreement allows Service Providers to access Covered Data and Information, and that Covered Data and Information will be used for testing and assessment purposes only.

3. Prohibition on Unauthorized Use or Disclosure of Covered Data and Information: Service Organization agrees that Service Providers will hold the Covered Data and Information in strict confidence. Service Providers shall not use or disclose any piece of Covered Data and Information that may be accessed except as permitted or required by the Agreement, as required by law, or as otherwise authorized in writing by UVM.

4. Safeguard Standard: Service Organization agrees that Service Providers will protect the Covered Data and Information according to commercially acceptable standards and no less rigorously than it protects its own Covered Data and Information.

5. Handling of Covered Data and Information: Service Providers will take no intentional action to make a copy of any piece of Covered Data and Information onto any computer or media without prior authorization by manager of the UVM department responsible for that data. In cases where information is copied onto any media – print, film, electronic, magnetic, optical, or otherwise – such Covered Data and Information will be carefully guarded by all Service Providers against unauthorized exposure and, once the issue has been resolved, Service Providers will destroy all copies of Covered Data and Information either through destructive erasure (magnetic and electronic media) or physical destruction (shredding other media, such as paper, CDs, DVDs, etc.).

6. Term and Termination:
   a. This Agreement shall take effect upon execution.

b. In addition to the rights of the parties established by the underlying Agreement, if UVM reasonably determines in good faith that any Service Provider has materially breached any of its obligations under this Agreement, UVM, in its sole discretion, shall have the right to:
   i. Exercise any of its rights to reports, access and inspection under this Agreement; and/or
   ii. Require Service Organization to submit to a plan of monitoring and reporting, as UVM may determine necessary to maintain compliance with this Agreement; and/or
   iii. Provide Service Organization with a fifteen (15) day period to cure the breach; and/or
   iv. Terminate the Agreement immediately if any Service Provider has breached a material term of this Agreement and cure is not possible.

c. Before exercising any of these options, UVM shall provide written notice to Service Organization describing the violation and the action it intends to take.

7. Subcontractors and Agents: If a Service Provider provides any Covered Data and Information which was received from, or created for UVM to a subcontractor or agent, then Service Organization shall require such subcontractor or agent to agree to the same restrictions and conditions as are imposed on Service Organization by this Agreement.

8. Maintenance of the Security of Electronic Information: Service Organization shall develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted Covered Data and Information received from, or on behalf of, UVM.

9. Reporting of Unauthorized Disclosures or Misuse of Covered Data and Information: Service Organization shall report to UVM any use or disclosure of Covered Data and Information not authorized by this Agreement or in writing by UVM. Service Organization shall make the report to UVM not more than one (1) business day after Service Provider learns of such use or disclosure. Service Organization's report shall identify:

   a. The nature of the unauthorized use or disclosure,
   b. The Covered Data and Information used or disclosed,
   c. Who made the unauthorized use or received the unauthorized disclosure,
   d. What Service Organization has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and
   e. What corrective action Service Organization has taken or shall take to prevent future similar unauthorized use or disclosure.

   Service Organization shall provide such other information, including a written report, as reasonably requested by UVM.

10. Indemnity: Service Organization shall defend and hold UVM harmless from all claims, liabilities, damages, or judgments involving a third party, including UVM's costs and attorney fees, which arise as a result of Service Organization's failure to meet any of its obligations under this Agreement.

11. Survival. The respective rights and obligations of Service Organization under Section 6 shall survive the termination of this Agreement.

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be duly executed in its name and on its behalf.

UNIVERSITY OF VERMONT		**SERVICE ORGANIZATION:**	
By:	_____	By:	_____
Title:	_____	Title:	_____
Signature:	_____	Signature:	_____
Date:	_____	Date:	_____

Appendix 3: Protected University Information Agreement (Non-Disclosure) for Data Transferred from UVM to an External Service Provider

The form on the following page (or a comparable form approved by the Office of General Counsel) must be signed by an appropriate representative of any external organization before any member of that organization can obtain non-public University information.

Protected University Information Agreement for Data Transferred to an External Service Provider

This agreement is hereby entered into, by and between _____

(hereinafter "Service Provider") and the University of Vermont (hereinafter "UVM") on _____(date). UVM and Service Provider mutually agree to the terms of this Agreement whereby UVM will provide the following data and information:

_____

_____

to Service Provider for the following purposes:

_____

_____

Such data and information shall be provided to Service Provider for a defined period, starting upon the execution of this agreement and ending no later than _____. If any conflict exists between the terms of this agreement and any prior agreement, the terms of this agreement shall govern.

1. Definition:
   Covered Data and Information will include all data and information provided by UVM to Service Provider specifically for the aforementioned purposes as well as any data and information that Service Provider may derive from such data and information.
2. Acknowledgment of Access to Covered Data and Information: Service Provider acknowledges that the Agreement allows the Service Provider access to Covered Data and Information, and that Covered Data and Information will be used for testing and assessment purposes only.
3. Prohibition on Unauthorized Use or Disclosure of Covered Data and Information: Service Provider agrees to hold the Covered Data and Information in strict confidence. Service Provider shall not use or disclose Covered Data and Information received from or on behalf of UVM except as permitted or required by the Agreement, as required by law, or as otherwise authorized in writing by UVM.
4. Safeguard Standard: Service Provider agrees that it will protect the Covered Data and Information it receives from or on behalf of UVM according to commercially acceptable standards and no less rigorously than it protects its own Covered Data and Information.
5. Return or Destruction of Covered Data and Information: Upon termination, cancellation, expiration or other conclusion of the Agreement, Service Provider shall:
   a. Return to UVM or, if return is not feasible, destroy all Covered Data and Information in whatever form or medium that Service Provider received from or created on behalf of UVM. This provision shall also apply to all Covered Data and Information that is in the possession of subcontractors or agents of Service Provider. In such case, Service Provider shall retain no copies of such information, including any compilations derived from and allowing identification of Covered Data and Information. Service Provider shall complete such return or destruction as promptly as possible, but not more than thirty (30) days after the effective date of the conclusion of this Agreement. Within such thirty (30) day period, Service Provider shall certify in writing to UVM that such return or destruction has been completed.

b. If Service Provider believes that the return or destruction of Covered Data and Information is not feasible, Service Provider shall provide written notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction is not feasible, Service Provider shall extend the protections of this Agreement to Covered Data and Information received from or created on behalf of UVM, and limit further uses and disclosures of such Covered Data and Information, for so long as Service Provider maintains the Covered Data and Information.

6. Term and Termination:
   a. This Agreement shall take effect upon execution.
   b. In addition to the rights of the parties established by the underlying Agreement, if UVM reasonably determines in good faith that Service Provider has materially breached any of its obligations under this Agreement, UVM, in its sole discretion, shall have the right to:
      i. Exercise any of its rights to reports, access and inspection under this Agreement; and/or
      ii. Require Service Provider to submit to a plan of monitoring and reporting, as UVM may determine necessary to maintain compliance with this Agreement; and/or
      iii. Provide Service Provider with a fifteen (15) day period to cure the breach; and/or
      iv. Terminate the Agreement immediately if Service Provider has breached a material term of this Agreement and cure is not possible.
   c. Before exercising any of these options, UVM shall provide written notice to Service Provider describing the violation and the action it intends to take.
7. Subcontractors and Agents: If Service Provider provides any Covered Data and Information which was received from, or created for, UVM to a subcontractor or agent, then Service Provider shall require such subcontractor or agent to agree to the same restrictions and conditions as are imposed on Service Provider by this Agreement.
8. Maintenance of the Security of Electronic Information: Service Provider shall develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted Covered Data and Information received from, or on behalf of, UVM.
9. Reporting of Unauthorized Disclosures or Misuse of Covered Data and Information: Service Provider shall report to UVM any use or disclosure of Covered Data and Information not authorized by this Agreement or in writing by UVM. Service Provider shall make the report to UVM not more than one (1) business day after Service Provider learns of such use or disclosure. Service Provider's report shall identify:
   a. The nature of the unauthorized use or disclosure,
   b. The Covered Data and Information used or disclosed,
   c. Who made the unauthorized use or received the unauthorized disclosure,
   d. What Service Provider has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and
   e. What corrective action Service Provider has taken or shall take to prevent future similar unauthorized use or disclosure.

   Service Provider shall provide such other information, including a written report, as reasonably requested by UVM.

10. Indemnity. Service Provider shall defend and hold UVM harmless from all claims, liabilities, damages, or judgments involving a third party, including UVM's costs and attorney fees, which arise as a result of Service Provider's failure to meet any of its obligations under this Agreement.
11. Survival. The respective rights and obligations of Service Provider under Section 6 shall survive the termination of this Agreement.

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be duly executed in its name and on its behalf.

UNIVERSITY OF VERMONT		**SERVICE ORGANIZATION:**	
By:	_____	By:	_____
Title:	_____	Title:	_____
Signature:	_____	Signature:	_____
Date:	_____	Date:	_____

Appendix 4: Protected University Information Addendum (Non-Disclosure) for Information Covered by the Gramm-Leach-Bliley Act

The form on the following page (or a comparable form approved by the Office of General Counsel) must be signed by an appropriate representative of any external organization before any member of that organization can be given access to University information that is protected by the Gramm-Leach- Bliley Act.

Protected University Information Addendum for UVM Information Covered by the Gramm-Leach-Bliley Act

This Addendum ("Addendum") amends and is hereby incorporated into the existing agreement known as _____ ("Agreement"), entered into by and between _____ (hereinafter "Service Provider") and the University of Vermont (hereinafter "UVM") on_____(date).

UVM and Service Provider mutually agree to modify the Agreement to incorporate the terms of this Addendum to comply with the requirements of the Gramm Leach Bliley Act ("GLB") dealing with the confidentiality of customer information and the Safeguards Rule. If any conflict exists between the terms of the original Agreement and this Addendum, the terms of this Addendum shall govern.

1. Definitions:
    a. *Covered Data and Information* includes *Student Financial Information* (defined below) required to be protected under the Gramm Leach Bliley Act (GLB), as well as any credit card information received in the course of business by the University, whether or not such credit card information is covered by GLB. Covered data and information includes both paper and electronic records.
    b. *Student Financial Information* is that information that the University has obtained from a customer in the process of offering a financial product or service, or such information provided to the university by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 C.F.R. §225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.
2. Acknowledgment of Access to Covered Data and Information: Service Provider acknowledges that the Agreement allows the Service Provider access to Covered Data and Information. Specifically, access to the following categories of Covered Data and Information is anticipated under the Agreement:

    _____

    _____

    _____
3. Prohibition on Unauthorized Use or Disclosure of Covered Data and Information: Service Provider agrees to hold the covered data and information in strict confidence. Service Provider shall not use or disclose Covered Data and Information received from or on behalf of UVM except as permitted or required by the Agreement or this Addendum, as required by law, or as otherwise authorized in writing by UVM.
4. Safeguard Standard: Service Provider agrees that it will protect the Covered Data and Information it receives from or on behalf of UVM according to commercially acceptable standards and no less rigorously than it protects its own Protected University Information.
5. Return or Destruction of Covered Data and Information: Upon termination, cancellation, expiration or other conclusion of the Agreement, Service Provider shall:
    a. Return to UVM or, if return is not feasible, destroy all Covered Data and Information in whatever form or medium that Service Provider received from or created on behalf of UVM. This provision shall also apply to all Covered Data and Information that is in the possession of subcontractors or agents of Service Provider. In such case, Service Provider shall retain no copies of such information, including any compilations derived from and allowing identification of Covered Data and Information. Service Provider shall complete such return

or destruction as promptly as possible, but not less than thirty (30) days after the effective date of the conclusion of this Agreement. Within such thirty (30) day period, Service Provider shall certify in writing to UVM that such return or destruction has been completed.

b. If Service Provider believes that the return or destruction of Covered Data and Information is not feasible, Service Provider shall provide written notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction is not feasible, Service Provider shall extend the protections of this Addendum to Covered Data and Information received from or created on behalf of UVM, and limit further uses and disclosures of such Covered Data and Information, for so long as Service Provider maintains the Covered Data and Information.

6. Term and Termination:
   a. This Addendum shall take effect upon execution.
   b. In addition to the rights of the parties established by the underlying Agreement, if UVM reasonably determines in good faith that Service Provider has materially breached any of its obligations under this Addendum, UVM, in its sole discretion, shall have the right to:
      i. exercise any of its rights to reports, access and inspection under this Addendum; and/or
      ii. require Service Provider to submit to a plan of monitoring and reporting, as UVM may determine necessary to maintain compliance with this Addendum; and/or
      iii. provide Service Provider with a fifteen (15) day period to cure the breach; and/or
      iv. terminate the Agreement immediately if Service Provider has breached a material term of this Addendum and cure is not possible.
   c. Before exercising any of these options, UVM shall provide written notice to Service Provider describing the violation and the action it intends to take.
7. Subcontractors and Agents: If Service Provider provides any Covered Data and Information which was received from, or created for, UVM to a subcontractor or agent, then Service Provider shall require such subcontractor or agent to agree to the same restrictions and conditions as are imposed on Service Provider by this Addendum.
8. Maintenance of the Security of Electronic Information: Service Provider shall develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted Covered Data and Information received from, or on behalf of, UVM.
9. Reporting of Unauthorized Disclosures or Misuse of Covered Data and Information: Service Provider shall report to UVM any use or disclosure of Covered Data and Information not authorized by this Addendum or in writing by UVM. Service Provider shall make the report to UVM not more than one (1) business day after Service Provider learns of such use or disclosure. Service Provider's report shall identify:
   a. the nature of the unauthorized use or disclosure,
   b. the Covered Data and Information used or disclosed,
   c. who made the unauthorized use or received the unauthorized disclosure,
   d. what Service Provider has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and
   e. what corrective action Service Provider has taken or shall take to prevent future similar unauthorized use or disclosure.

   Service Provider shall provide such other information, including a written report, as reasonably requested by UVM.

10. Indemnity. Service Provider shall defend and hold UVM harmless from all claims, liabilities, damages, or judgments involving a third party, including UVM's costs and attorney fees, which arise as a result of Service Provider's failure to meet any of its obligations under this Addendum.
11. Survival. The respective rights and obligations of Service Provider under Section 6 shall survive the termination of this Agreement.

IN WITNESS WHEREOF, each of the undersigned has caused this Addendum to be duly executed in its name and on its behalf.

UNIVERSITY OF VERMONT		**SERVICE ORGANIZATION:**	
By:	_____	By:	_____
Title:	_____	Title:	_____
Signature:	_____	Signature:	_____
Date:	_____	Date:	_____